REMARKS

The present application was filed on April 5, 2001 with claims 1-20. In the outstanding Office Action, the Examiner: (i) withdraws the allowability of claims 1, 3-8, 10, 12-17, 19 and 20; and (ii) rejects claims 1, 3-8, 10, 12-17, 19 and 20 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,539,479 to T.J. Wu (hereinafter "Wu").

Regarding the §102(e) rejection of claims 1, 3-8, 10, 12-17, 19 and 20 based on Wu, Applicant traverses the rejection for at least the following reasons. It is well-established law that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Applicant asserts that the rejection based on Wu does not meet this basic legal requirement, as will be explained below.

The present invention, for example, as recited in independent claim 1, comprises a method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation. The method comprises the steps of one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, whereby the other party may perform the inverse group operation on m and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and calculate the shared secret g^{xy}. Independent claims 10 and 19 recite similar limitations in accordance with apparatus and article of manufacture aspects of the invention. Independent claims 8, 17 and 20 respectively recite similar limitations as claims 1, 10 and 19 from the perspective of the "other party."

While Wu is a password-only authentication protocol, Wu does not teach or suggest each and every element of the claimed invention. For example, Wu does not teach or suggest "any portion of a result associated with the function that is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.

2

The Examiner appears to suggest (at page 3 of the Office Action) that Wu discloses randomizing the part of a result lying outside a group, and subsequently removing that randomization. However, Wu does not teach or suggest anything like that.

The only randomness that Wu discloses is when client computer ("Carol," as referred to in Wu) generates a random number, for example, w_s (in the log-in procedure of FIG. 2), and the server ("Steve," as referred to in Wu) generates a random number u, from which the server attempts to authenticate the client computer, see column 8, line 43, through column 9, line 15. Columns 10 through 12 of Wu describe variants of the protocol. However, again, the only randomness is with respect to certain values generated by either the server (e.g., random string r_1 in step 210A) or the client computer (e.g., random string r_2 in step 230).

Thus, in Wu, there is no notion of any result being "outside of a group." Hence, it is not possible for Wu to disclose randomizing something outside of a group. Therefore, it is quite clear that Wu fails to teach or suggest "any portion of a result associated with the function that is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.
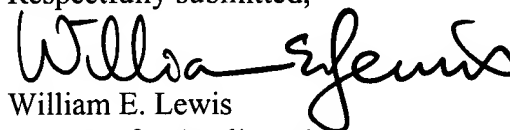
For at least the above reasons, Applicant asserts that claims 1, 3-8, 10, 12-17, 19 and 20 are patentable over Wu.

In addition, Applicant asserts that the various rationales given in the Office Action for rejecting the dependent claims of the application are also deficient and, thus, Applicant asserts that such claims contain separately patentable subject matter in their own right.

While not expressly stated in the Office Action with respect to claims 2, 9, 11 and 18, it is assumed that such objected-to claims would be allowable if rewritten in independent form. Applicant reserves the right to do so, pending the outcome of this present response.

In view of the above, Applicant believes that claims 1-20 are in condition for allowance, and respectfully requests withdrawal of the §102(e) rejection.

Respectfully submitted,

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

Date: January 20, 2006

3